العنوان:	الحماية القانونية لقواعد البيانات في نظم المعلومات
المصدر:	أعمال ندوات (مكافحة الجريمة عبر الانترنت) وورشة عمل (أمن المعلومات والتوقيع الألكتروني) - المنظمة العربية للتنمية الإدارية - مصر
المؤلف الرئيسي:	الألفي، محمد محمد
محكمة:	نعم
التاريخ الميلادي:	2010
مكان انعقاد المؤتمر:	القاهرة
الهيئة المسؤولة:	المنظمة العربية للتنمية الإدارية
الصفحات:	181 - 202
رقم MD:	125070
نوع المحتوى:	بحوث المؤتمرات
قواعد المعلومات:	science, HumanIndex
مواضيع:	الانترنت، الحماية القانونية، قواعد البيانات، جرائم المعلومات، الجرائم الإلكترونية، أمن المعلومات، القوانين و التشريعات، المعاملات الرقمية، العقود الإلكترونية، التجارة الإلكترونية، البنوك الإلكترونية، التوقيع الإلكتروني، الحكومة الإلكترونية، حروب المعلوماتية، الشبكات العسكرية، الشبكات الاقتصادية، شبكات الطاقة الكهربائية، الجدران النارية، الشبكات الافتراضية، المصنفات الرقمية
رابط:	http://search.mandumah.com/Record/125070

الحماية القانونية لقواعد البيانات

في نظم المعلومات*

إعداد

المستشار/ محمد محمد الألفي

رئيس المحكمة

عضو المجموعة التأسيسية للجمعية الدولية لقانون الإنترنت

* ورقة عمل مقدمة في ندوة "أمن وحماية نظم المعلومات في المؤسسة العربية"، القاهرة – جمهورية مصر العربية، يونيو 2007.

مقدمة:

اتجه الفكر العالمي ممثلاً في الحكومات والمنظمات والتجمعات الدولية إلى تحقيق ذلك بما يسمى بالحكومة الإلكترونية بدءاً بتوفير المعلوماة إنتهاءً بإمكانية تقديم الخدمات من خلال شبكات الأتصال الإلكترونية المختلفة، وقد نتج عن تلك الرؤية عدة مشاريع تستخدم شبكات الهاتف وشبكات الحاسب الآلية، وتركز هذه المشاروعات على تنفيذ عدد من مستويات تقديم الخدمة بدءاً من مجرد نشر المعلومات عن الخدمة وحتى مستوى تقديم الخدمة بكاملها بصورة إلكترونية.

وفي إطار تنمية تكنولوجيا المعلومات والاتصالات ومواكبة التطور الهائل في استخدامها في كافة المجالات والأنشطة، تم التفكير في تطبيق التوقيع الإلكتروني، والذي تكمن أهميته في زيادة مستوى الأمن والخصوصية في التعاملات، نظراً لقدرة هذه التقنية على حفظ سرية المعلومات والرسائل المرسلة وعدم قدرة أي شخص أخر على الإطلاع أو تعديل أو تحريف الرسالة، كما يمكنها أن تحدد شخصية وهوية المرسل والمستقبل إلكترونيا للتأكد من مصداقية الشخصية مما يسمح بكشف التحايل أو التلاعب.

إن إتاحة أستخدام التوقيع الإلكتروني تدعم التحول إلى عالم لا ورقي، يامن فيه كل متعامل على أمواله ومصالحه. كما أن التوسع في استخدام الخدمات التوقيع الإلكتروني يرفع كفاءة العمل الإداري ويساعد علي الارتقاء بمستوي أداء الخدمات الحكومية بما يتفق مع إيقاع العصر، ومن شأنه أن يضيف إلى المزايا التنافسية في ظل النظام التجاري العاملي الجديد، والذي أصبحت المعاملات الإلكترونية سمة من سماته وعلامة دالة عليه.

مفاهيم الدراسة:

يأتي دور الفقه لوضع إطار من خلاله يتم التعريف بكل المصطلحات المرتبطة بالتنظيم القانوني للعام الإفتراضي:

١. **مفهوم قانون الإنترنت:**

هو ذلك الفرع الجديد من فروع القانون الذي يتولى التنظيم القانوني للإنترنت ... ولقد تم تقسيم قانون الإنترنت إلى خمسة موضوعات كبرى هي على التوالي:

- التخزين الرقمي.
- قواعد البيانات.
- التجارة الإلكترونية.
- الإجرام عبر الإنترنت.
- والمعاملات الرقمية.

٢. **المعاملات الرقمية:**

وهذا القسم من الأقسام المعاصرة لقانون الإنترنت يتناول كافة المعاملات التي تندرج في إطار الحياة المدنية للفرد في علاقاته مع العالم الإفتراضي، ومن ذلك موضوعات شتى مثل الحقوق والحريات والألتزامات الرقمية والملكية الفكرية عبر الإنترنت والعقوم الرقمية ... إلخ. فهذا القسم يشكل تلك الرؤية المباشرة في علاقة الفرد بتكنولوجيا المعلومات موضوعاً، وهو قسم نابع من مصداقية فكرة أن الأنترنت ليست مجرد تقنية أو تكنولوجيا فقط وإنما في الحقيق هي تقنية إنسانية يجب أن يتفاعل معها الإنسان أو الفرد في كل مكان [١].

٣. **العقد الإلكتروني:**

هو إتفاق يتلاقى فيه الإيجاب والقبول على شبكة الإنترنت وذلك بوسيلة مسموعة أو مرئية ولا يختلف العقد الإلكتروني عن العقود التقليدية سوى في طريقة أنعقاد العقد.

٤. **التجارة الإلكترونية (E-commerce):**

هي تنفيذ وإدارة الأنشطة التجارية المتعلقة بالبضاعة والخدمات بواسطة تحويل المعطيات عبر شبكة الإنترنت أو الأنظمة التقنية الشبيهة.

---

(١) د. عمر بن يونس، محاضرة بعنوان نظم الشراء الإلكتروني في المؤسسات الحكومية في المنظمة العربية للتنمية الإدارية، 2006.

٥. **البنك الإلكتروني:**

هو النظام الذي يتيح للعميل الوصول إلى حساباته أو أية معلومات يريد الحصول عليها وعلى مختلف الخدمات المصرفية والمنتجات المصرفية من خلال شبكة معلومات يرتبط هب جهاز الحاسوب الخاص به أو أية وسيلة أخرى.

٦. **التوقيع الإلكتروني:**

هو التوقيع اللازم لأتمام تصرف قانوني يحدد الشخص الذي يجريه. وهو يعبر عن رضى الأطراف بالألتزامات الناشئة عن هذا التصرف يوضع على محرر إلكتروني ويتخذ حروف أو أرقام أو رموز إو إشارات أو غيرها ويكون له طابع متفرد يسمح بتحديد شخص الموقع ويميّزه عن غيره.

٧. **الحكومة الإلكترونية** [٢]:

هي قدرة القطاعات الحكومية المختلفة على تقديم الخدمات والمعلومات الحكومية التقليدية للمواطنين بوسائل إلكترونية وبسعة وقدرة متناهيتين وبتكاليف ومجهود أقل وفي أي وقت ومن خلال موقع واحد على شبكة الإنترنت.

٨. **المصنف الرقمي:**

هو أي مصنف إبداعي عقلي ينتمي إلى بيئة تقنية المعلومات وفق المفهوم المتطور للأداء التقني.

ويتضمن هذا العمل عدة محاور ترتبط بالتوسع في إستخدامات نظم وتطبيقات وخدمات المعلومات الرقمية الحكومية التي تتاح على شبكات المعلومات التي صارت تتسم بالإعتمادية، وقابليتها للتعرض للضرر والخطر، وحاجتها لأكتساب الثقة في التعامل معها من قبل المواطنين؛ وأمن نظم المعلومات وتطبيقاتها وخدماتها في بيئة المصالح والمنظمات الحكومية الرقمية التي يجب أن تمثل حماية سريتها وسلامتها وتوافرها فيما يتصل بالتهديدات المطلوب مواجهتها والاعتبارات العامة التي تشكل معالم شفافيتها من العمليات والبشر والتكنولوجيا والثقافة المؤسسية المتاحة؛

---

(2) www.arriyadh.com/Gov/index.asp - 98k.

ومتطلبات الأمن الطبيعي والمنطقي والفني والسيكولوجي للمعلومات التي تحدد عمليات التحقق من الأمن المستهدفة (التعريف، الأعتماد، افدارة والمراجعة)، وتفهم استخدام نظم المعلومات، ومحاسبة إدارة الأمن وتنفيذ أدوات ومنتجات الأمن؛ واعتبارات وأبعاد أمن المعلومات؛ وتوجيهات ومعايير أمن نظم المعلومات من حيث غرضها العام ومجالها وتعاريفها وأهدافها والمبادئ الخاصة بأمن المعلومات؛ وتنفيذ نظم أمن وشفافية المعلومات المرتبط بتطوير السياسة الخاصة بنظام الأمن والتعليم والتدريب المصاحب لتطوير النظام وتبادل المعلومات والتعاون في المعلومات الأمنية لنظم المعلومات وتطبيقاتها وخدماتها. ويختتم هذا العمل بالخلاصة التي تتضمن النتائج والتوصيات المتوصل إليها. كل هذه الأستخدامات الرقمية من المؤسسات وما بها من نظم معلوماتية تحتاج إلى حماية حال تعاماً هذه المؤسسات بنظام المعاملات الرقمية وهو ما ستلقي الضوء عليه في بحثنا:

أمن المعلومات ماهيتها وعناصرها وإستراتيجياتها [٣]:

١. ما المقصود بأمن المعلومات وما هي عناصره؟

أمن المعلومات:

- **من زاوية أكاديمية:** هو العلم الذي يبحث في نظريت وإستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الأعتداء عليها.
- **ومن زاوية تقنية:** هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية.
- **ومن زاوية قانونية:** هو محل دارسات وتدابر حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الأعتداء عليها أو أستغلال نظمها في إرتكاب الجريمة، وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تسهدف المعلومات ونظمها (جرائم الكمبيوتر والإنترنت).

---

(3) www.arablaw.net

٢. عناصر أمن المعلومات:

أن أغراض أبحاث وإستراتيجيات ووسائل أمن المعلومات- سواء من الناحية التقنية أو التدابير التشريعية هو ضمان توفر العناص التالية لأية معلومات يراد توفير الحماية الكافية لها:

- **السرية أو الموثوقية:** وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك.
- **التكاملية وسلامة المحتوى:** التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به وبشكل خاص لن يتم تدمير المحتوى أو تغيره أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع.
- **إستمرارية توفير المعلومات أو الخدمات:** التأكد من إستمرار عمل النظام المعلوماتي وإستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية وإن مستخدم المعلومات لن يتعرض إلى منع أستخدامه لها أو دخوله إليها.
- **عدم إنكار التصرف المرتبط بالمعلومات ممن قام به:** ويقصد به ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها إنكار إنه هو الذي قام بهذا التصرف، بحيث تتوفر قدرة إثبات أن تصرفاً ما قد تم من شخص ما في وقت معين.

ليس كل المعلومات تتطلب السرية وضمان عدم الإفشاء، وليس كل المعلومات في منشأة واحدة بذات الأهمية من حيث الوصول لها أو ضمان عدم العبث بها، لذا يجب توضيح بعض النقاط قبل التعرض للحماية القانونية:

- وإذا كان النظام يتبادل رسائل إلكترونية يخشى على بياناتها من الإفشاء، تكوين تقنيات التشفير مطلوبة بالقدر المناسب.

لكن لا يقبل مثلاً على جهاز كمبيوتر خاص غير مرتبط بشبكة عامة أن:

- توضع أنواع متعددة من الجدران النارية.
- أو أن يوضع على أحد مواقع الإنترنت وسائل تعريف متعددة لشخص المستخدم، ككلمة السر والبصمة الإلكترونية والبصمة الصوتية.
- وأن يخضع نظام الموقع إلى عدد مبالغ به من الفلترات والجدران النارية.
- وتشفير طويل المدي لكافة البيانات الموجودة عليه والمتبادلة عبره
- وأيضاً لا يقبل موقع أمني يضع بيانات سرية للغاية مجرد الأقتصار على كلمة سر الدخول للنظام. بمعنى ان إجراءات الحماية تنطلق من إحتياجات الحماية الملائمة للحماية من أختراق الشبكات الإلكترونية في الدول المتقدمة [٤].

في فجر الثورة الرقمية، في منتصف العقد الماضي، انتبه الغرب إلى قضية الإرهاب الإلكتروني ومخاطره، حيث قام الرئيس الأمريكي "بيل كلينتون" في العام 1996 بتشكيل لجنة حماية منشآت البنية التحتية الحساسة www.nipc.gov. وكان أول أستنتاج لهذه الهيئة هو أن مصادر الطاقة الكهربائية والاتصالات إضافة إلى شبكات الكمبيوتر ضرورية بشكل قاطع لنجاة الولايات المتحدة، وبما أن هذه المنشآت تعتمد بشكل كبير على المعلومات الرقمية، فإنها ستكون الهدف الأول لأية هجمات إرهابية تستهدف أمن الولايات المتحدة وفي أعقاب ذلك، قامت كافة الوكالات الحكومية في الولايات المتحدة، بإنشاء هيئاتها ومراكزها الخاصة، للتعامل مع إحتمالات الإرهاب الإلكتروني. فقامت وكالة الأستخبارات المركزية بإنشاء مركز حرب المعلوماتية، ووظفت ألفاً من خبراء أمن المعلومات، وقوة ضاربة على مدى 24 ساعة لمواجهة الإرهاب الإلكتروني. وقامت القوات الجوية الأمريكية بإتخاذ خطوات مماثلة،

---

(4) www.wikipedia.org/wiki/- 50k.ar جريمة رقمية

ومثلها المباحث الفيدرالية. كما تقوم قوات الأمن في أوروبا، وخصوصاً الدول التابعة لحلف الأطلسي، بإتخاذ إجراءات مماثلة.

أشكال حروب المعلوماتية:

وكما هي الحال في أية حرب، فإن الجيوش المتصارعة تستهدف دوماً ثلاثة عناصر أساسية من أجل كسب المعركة؛ وهي العناصر العسكرية، والأقتصادية، والسياسية أو بكلمات أخرى إدارة الشعب. وفي عالم حروب المعلومات تجد العناصر الثلاث نفسها وعلى رأسها مراكز القيادة والتحكم العسكرية، والبنوك والمؤسسات المالية، ومؤسسات المنافع كمؤسسات المياه والكهرباء وذلك لإخضاع إدارة الشعوب.

الهجمات على الشبكات العسكرية:

تستهدف هذه النوعية من الهجمات عادة، الأهداف العسكرية غير المدنية، والمرتبطة بشبكات المعلومات. وهذا النوع من الهجمات نادر الحدوث عادة لعدة أسباب أولها هو أنه يتطلب معرفة عميقة بطبيعة الهدف، وطبيعة المعلومات التي يجب النفاذ إليها، وهي معرفة لا تمتلكها إلا الحكومات، إضافة إلى أن الحكومات تقوم عادة بعزل المعلومات العسكرية الحساسة عن العالم، ولا تقوم بوصل الأجهزة التي تحملها بالعالم الخارجي بأي شكل من الأشكال. ولكن يبقى الحذر واجباً من عمليات التخريب الداخلية، ومن هنا تأتي ضرورة وضع نظم موثوقة للتحقق من شخصيات المستخدمين، والتحديد الدقيق لطبيعة المعلومات التي يُسمح بالنفاذ إليها. ومن السيناريوهات التي تمثل هذا النوع من الهجمات، هو النفاذ إلى النظم العسكرية وأستخدامها لتوجيه جنود العدو إلى نقطة غير آمنة قبل قصفها بالصواريخ مثلاً.

الهجمات على الشبكات الأقتصادية:

أصبح الأعتماد على شبكات الكمبيوتر شبه مطلق في عالم المال والأعمال، مما يجعل هذه الشبكات، نظراً لطبيعتها المترابطة، وإنفتاحها على العالم، هدفاً مغرياً للعابثين والهكرة. ومما يزيد من إغراء الأهداف الإقتصادية والمالية هو أنها تتأثر بشكل كبير بالإنطباعات السائدة والتوقعات، والتشكيك في صحة هذه المعلومات، أو تخريبها بشكل بسيط يمكن أن يؤدي إلى نتائج مدمرة، وإضعاف الثقة في النظام الإقتصادي. ولذلك فإن الهجمات ضد نظم

المعلومات الإقتصادية يمكن لها أن تكون من مؤذية جداً. ومن الأمثلة على الهجمات الإقتصادية هي العملية التي قامت بها مجموعه من الهكرة، تُعرف بإسم نادي الفوصى، في عام 1997، حيث قام هؤلاء بإنشاء بريمج تحكم بلغة آكتف إكس مصمم للعمل عبر إنترنت ويمكنه خداع برنامج كويكن Quicken المحاسبي بحيث يقوم بتحويل الموال من الحساب المصرفي للمستخدمين. وباستخدام هذا البريمج أصبح بإمكان هؤلاء الهكرة سرقة الأموال من أرصدة مستخدمي برنامج كويكن في جميع أنحاء العالم. وهذه الحالة هي مثال واحد فقط على الطرق التي يمكن بها مهاجمة شبكات المعلومات الأقتصادية وإستغلالها، وهي طرق يمكن أن يكون لها آثار مدمرة على المجتمعات.

الهجمات على شبكات الطاقة الكهربية:

أصبح الأعتماد على شبكات المعلومات، وخصوصاً في الدول المتقدمة، من الوسائل المهمة لإدارة نظم الطاقة الكهربية. ويمكن لهجمات على مثل هذا النوع من شبكات المعلومات أن تؤدي إلى نتائج خطرة وحقيقية، وخصوصاً في ظل أعتماد الإنسان المعاصر على الطاقة الكهربائية. ومن الإحصائيات البشعة التي يمكن لها أن تدلنا على فعالية مثل هذا النوع من الهجمات هي تلك المتعلقة بالهجمات على العراق خلال حرب الخليج الثانية. حيث تشير مصادر كلية الحرب الأمريكية إلى أن ضرب مولدات الطاقة الكهربائية العراقية أدى بشكل غير مباشر إلى موت ما بين 70 إلى 90 ألف مواطن عراقي كنتيجة مباشرة لعدم توافر الطاقة الكهربائية. ولذلك، فإن شبكات المعلومات المرتبطة بشكل مباشر أو غير مباشر بشكبات الطاقة الكهربائية تعتبر من الأهداف الأولى التي قد يستهدفها الإرهاب الإلكتروني.

ولا يتوقف الأمر عند هذا الحد، حيث أن هنالك الكثير من الهداف الأخرى، التي يمكن بواسطتها للهكرة المتمكنين أن يشيعوا الفوضى في الحياة المدنية. فهنالك مثلاً شبكات المعلومات الطبية، والتي يمكن لمهاجمتها، وأختراقها، ومن ثم التلاعب بها أن يؤدي إلى خسائر في أرواح المرضى من المدنيين. وهنالك حالات في العالم الغربي حيث قام الهكرة بالنفاذ إلى سجلات المستشفيات والتلاعب بسجلات المرضى بشكل أدى إلى حقن هؤلاء بأدوية وعلاجات كانت مميتة بالنسبة لهم. وحتى لو افترضنا أن شبكات المعلوماتية الخاصة بالمؤسسات الطبية منعية، فإن

رسالة واحدة تُنشر مثلاً بالبريد الإلكتروني، مفادها أن هنالك دماء ملوثة في المستشفيات وما إلى ذلك، يمكن لها أن تحدث آثار مدمرة على الصعيد الإجتماعي.

سبل الحماية:

(١)تأمين خطوط الدفاع الأمامية بأستخدام تطبيقات الجدران النارية(٥):

وتقوم هذه الفئة من التطبيقات بتأمين المنافذ ports التي تحصل من خلالها التطبيقات على خدمات إنترنت. وهذه المنفاذ تُحدد برمجياً ضمن نظم التشغيل أو التطبيقات المستخدمة. وفي كثير من الحيان لا يستعمل المستخدم كافة هذه المنافذ مما يجعله يسهو عن تأمينها وحمايتها، مما يشكل فرضة مثالية للهكرة للنفاذ إلى النظم. وتعمل برمجياد الجدران النارية كمصفاة تمنع وصول الطلبات المشبوهة إلى الأجهزة المزودة، وذلك بالأعتماد على مجموعة من السياسات policies التي يحدد بموجبها مدراء الشبكة طبيعة المعلومات التي يُسمح للعاملين بالمؤسسة النفاذ إليها. وضمن فئة الجدران النارية يوجد صنفان، الول هو الجدران النارية المؤسسية، والتي تقوم بحماية تطبيقات المؤسسات على مستوى الأجهزة المزودة، وبالتالي الأجهزو المرتبطة بهذه النظم المزودة، طالما بقيت مرتبطة بالشبكة. ولكن في عصر المستخدم النقال، والعمل من المنزل، حيث لا يوجد جدران نارية وأجهزة مزودة، تكتسب الجدران النارية الشخصية أهمية خاصة. وقد بدأ مدراء المعلوماتية في الغرب مؤخراً يقومون بتثبيت الجدران النارية الشخصية على الأجهزو المحمولة التي يستخدمها العاملون في المؤسسات. ويجب ان نذكر هنا أن الجدران النارية ليست الحل السحري الذي يوفر الأمن الشامل، وأنه يجب استخدام طبقات أخرى من الأمن تتجاوز الخطوط الأمامية.

(٢)تأمين حسابات المستخدمين ونظم التحقق من الهوية:

(5) http://www.nipc.gov/cybernotes/cybernotes.htm

رغم وجود العديد من تقنيات التحقق من الهوية وخصوصاً أساليب التحقق البيولوجي من الهوية (بالإعتماد على الصفات الشخصية والسمات الجسدية للأشخاص)، تبقى كلمات السر وأسماء المستخدمين هي الوسيلة الأكثر شيوعاً للتحقق من الهوية، رغم أن هذه الأساليب تصبح أضعف وأضعف بتطور التقنيات التي يستخدمها الهكرة لكشفها وخرقها. ومع ذلك، فهنالك الكثير من الوسائل التي يمكن أستخدامها للحد من قدرة الهكرة على إختراق وإكتشاف هذه الرموز. وتعتمد هذه الوسائل أساساً على تحديد حقوق نفاذ المستخدمين إلى الشبكات، وحصرها بما يحتاجه كل مستخدم. ولكن هذه التقنيات، ورغم قوتها، ليست حلولاً سحرية، إذ أنها تتطلب الكثير من المهارة والتخطيط الواعي قبل تطبيقها كي تحقق النجاح. وتتكون نظم التحقق من الهوية من ثلاث تقنيات هامة هي خدمات الدلة Directory Services، وهيكلية المفاتيح العامة Public Key Infrastructure، والشبكات الإفتراضية الخاصة Virtual Private Networks. وتشكل هذه التقنيات الثلاث هيكلية شاملة للتحقق من هوية المستخدمين، وضمان تحديد حقوق النفاذ.

(٣)خدمات الدلة:

برمجيات خدمات الأدلة هي عبارة عن قواعد بيانات خاصة، ذات مستو عالٍ من الأمان عادة، ومصممة لجمع، وإدارة المعلومات المتعلقة بمستخدمي الشبكات. ولا يقتصر دور هذه البرمجيات على جميع كلمات السر وأسماء المستخدمين، بل تطورت اليوم لتشمل السمات البيولوجية للمستخدمين. ويتم إستخدام هذه المعلومات لتحديد حقوق المستخدمين على الشبكة بجميع مكوناتها كالتطبيقات، والأجهزة الخادمة، والمجلدات، وحتى شكل الشاشة التي يستعملها المستخدم. وتُدار هذه كلها بشكل مركزي من مكتب مدير الشبكة دون الحاجة للقيام بأية زيارات إلى الأجهزة أو المستخدمين. وتعتبر شركة نوفيل Novell الشركة الرائدة في هذا المجال بمجموعتها الكبيرة من التطبيقات الموجهة لهذا الغرض.

(٤)تقنية المفتاح العام:

تعتمد هذه التقنية على تقنيات تشفير البيانات، أو بعثرتها Scrambling اعتماداً على علاقات رياضية خاصة تجمع ما بين مفتاحين (أو بالأحرى كلمتين سريتين) أحدهما عام والآخر خاص. فعند إرسال رسالة Message (كلمة رسالة هنا تشمل أي نوع من المعلومات المتناقلة بين النظم الإلكترونية بما في ذلك الأوامر التي تتناقلها التطبيقات بين بعضها البعض) يقوم التطبيق الموجود على جهازي بتشفيرها، أو بعثرة بياناتها، بإستخدام كلمة سر غير معروفة لأحد سواي، ثم تشفيرها ثانية بالمفتاح العام للمشتقبل. والسبيل الوحيد الذي يمكن به المستقبل أن يتعامل مع هذه الرسالة بتمثل في فك تشفيرها، أو إعادة ترتيب بياناتها، بإستخدام مفتاحه الخاص (أو كلمته السرية) أولاً، ومن ثم إستخدام مفتاحي العام لفك شيفرتي الخاصة. وتقوم هيئات عالمية وشركات خاصة بإصدار شهادات رقمية للمصادفة على صحة هذه المفاتيح ومنها شركات مثل RSA أو VeriSign (فيري ساين). ويمكن الحصول على المزيد من المعلومات عن تقنية المفتاح العام بالتوجه إلى الموقع www.pkiforum.org

(٥)الشبكات الإفتراضية الخاصة:

لا توجد طريقة أكثر أمناً من الشبكات الإفتراضية الخاصة للتحكم في الأشخاص الذين يمكنهم النفاذ إلى شبكتك. وتتلخص هذه التقنية بإقامة قناة خاصة وسيطة عبر الشبكة العامة، لا ينفذ من خلالها إلا من يقوم بتحديده مدير الشبكة. وفي هذه الحالة يمكن للمستخدمين المعينين النفاذ إلى الشبكة عبر الإنترنت وإسقاك الحزم الواردة من أية جهات أخرى غير هؤلاء المستخدمين. وتعتمد هذه التقنيات على بروتوكولات أتصالات آمنة وخاصة أهمها برتوكول IPSec والذي يعتمد شفرات بطول 128 بت.

(٦)أمن البرمجيات:

بالطبع، لا يمكن اعتبار أية سياسة أمنية شاملة، ما لم يتم الأعتناء بامن البرمجيات المستخدمة على الشبكة. وللأسف، فإن هذه هي النقطة الأصعب، حيث يجب إجبار، أو تثقيف المستخدمين، ليقوموا بتحديث برمجياتهم واعتماد كافة التصليحات التي تعتمدها الشركات المنتجة. وضمن المؤسسات يجب أن يعي مدراء الشبكة أهمية تحديث البرمجيات وتطبيق التصليحات بشكل مستمر كي يضمنوا شمولية السياسات الأمنية

المعتمدة لديهم. وبالطبع يصعب متابعة جميع هذه التصليحات من خلال إنترنت حيث إنها تتطلب الكثير من الوقت للمتابعة. وهناك مصدر للحكومة الأمريكية، وهو عبارة عن مجلة تُنشر كل أسبوعين يتم من خلالها نشر قائمة بجميع العثرات والثغرات المكتشفة في البرمجيات وطرق تصليحها، وهي موجودة على العنوان ( ) وهو مرجع ممتاز لهذا الغرض.

التدابير التشريعية العربية لحماية المعلومات والمصنفات الرقمية [٦]:

النظام القانوني لحماية المصنفات الرقمية:

ما هو المصنف الرقمي من الوجهة القانونية، تعاملت النظم والدراسات القانونية والقواعد التشريعية مع مصنفات المعلوماتية بوصفها تنتمي إلى بيئة الكمبيوتر.

- **وقد شملت هذه المصنفات ثلاثة أنواع من المصنفات:**
  - البرمجيات.
  - وقواعد البيانات.
  - وطبوغرافيا الدوائر المتكاملة.
- وهي مصنفات جاءت وليدة علوم الحوسبة مستقلة عن علوم الاتصال وتبادل المعطيات وشبكات المعلومات
- ومع ظهور شبكات المعلومات ظهرت أنماط جديدة من المصنفات أو عناصر مصنفات تثير مسألة الحاجة إلى الحماية القانونية وهي:
  - أسماء النطاقات أو الميادين أو المواقع على الشبكة Domain Names.
  - وعناوين البريد الإلكتروني.
  - وقواعد البيانات على الخط التي تضمها مواقع الإنترنت، تحديداً ما يتعلق بالدخول إليها وإسترجاع البيانات منها والتبادل المتعلق بمحتواها الحاصل على الخط.

---

[6] www.arabcin.net/arabic/5nadweh/pivot_7/arabic_arrangement.htm - 66k

- وهو تطور لمفهوم قواعد البيانات السائدة قبل إنتشار الشبكات التي كان مفهوماً أنها نخزنة داخل النظام أو تنقل على واسطة مادية تحتويها. ومادة أو محتوى موقع الإنترنت من نصوص ورسوم وأصوات ومؤثرات حركية (يطلق على المؤثرات الصوتية والحركية لوسائط المتعددة– Multimedia).
- فالمصنف الرقمي يشمل كافة المصنفات المتقدمة:
  - فبرنامج الكمبيوتر من حيث البناء والأداء مصنف رقمي.
  - وقاعد البيانات من حيث آلية ترتيبها وتبويبها.
  - والأوامر التي تتحكم بذلك تنتمي إلى البيئة الرقمية.
  - وذات القول يرد بالنسبة لكافة العناصر المتقدمة.
- وبالتالي فالمصنف الرقمي هو أي مصنف إبداعي عقلي ينتمي إلى بيئة تقنية المعلومات وفق المفهوم المتطور للأداء التقني.
- فتتمثل المصنفات الرقمية:
  - في الكمبيوتر ببرامج الحاسوب وبقواعد البيانات وبالدوائر المتكاملة.
  - أما في بيئة الإنترنيت فتتمثل بأسماء نطاقات أو مواقع الإنترنت، وبمحتوى المواقع من مواد النشر الإلكتروني نصوصاً وصوراً ومواد سمعية ومرئية (الوسائط المتعددة).

برامج الحاسوب:

إن البرمجيات هي الكيان المعنوي لنظام الكمبيوتر دونها لا يكون ثمة أي فائدة للمكونات المادية من الأجهزة والوسائط وهي بوجه عام تنقسم من الزواية التقنية إلى:

- برمجيات التشيل المناط بها إتاحة عمل مكونات النظام معاً وتوفير بيئة عمل البرمجيات التطبيقية.
- وتمثل البرمجيات التطبيقية النوع الثاني من أنواع البرمجيات وهي التي تقوم بمهام محددة كبرمجيات معالجة النصوص أو الجداول الحسابية أو الرسم أو غيرها.

فالخوارزميات هي العناصر والرموز الرياضية التي يتكون منها بناء البرنامج وهي كالأفكار والحقائق العلمية ليست محل حماية لأنها ليست موضعاً للأستثمار (مادة 2/9 من إتفاقية تربس) لكنها متى ما نظمت على شكل أوامر إبتكارية لتحقيق غرض معين أصبحنا أمام برنامج، وهو بهذا الوصف إن توفرت له عناصر الجدة والإبتكار والأصالة محل للحماية شأنه شأن أي من مصنفات الملكية الفكرية الأدبية الأخرى.

وقد أثارات برامج الحاسوب جدلاً واسعاً بشأن طبيعتها وموضع حمايتها من بين تشريعات الملكية الفكرية، وترددت الآراء بين:

- من يدعو لحمايتها عبر نظام براءات الأختراع لما تنطوي عليه من سمة الأستغلال الصناعي وأتصالها العضوي بمنتج مادي صناعي.
- وبين من ذهب إلى حمايتها عبر نظام الأسرار التجارية إذ تنطوي في الغالب على سر تجاري يتجلى بالأفكار التي انبنى عليها أو الغرض من ابتكارها.
- وبين داع إلى حمايتها عن طريق الشروط العقدية التي تجد مكانها في رخص الأستخدام أو إتفاقيات الأستغلال .
- لكن كافة هذه الآراء لم تصمد أما الرأي الذي وجد في البرمجيات عملاً إبتكارياً أدبياً، يضعها ضمن نطاق مصنفات الملكية الأدبية (حق المؤلف) إذ هي أفكار وترتيب لخوارزميات تفرغ ضمن شكل إلتكاري إبداعي، وسماتها وصفاتها المميزة تتقابل مع عناصر الحماية لمصنفات الملكية الأدبية.

ولاسيما بعد أن وضعت منظمة الوايبو القانون النموذجي أو الإرشادي عام 1978 بشأن حماية البرمجيات وبعد سلسلة أجتماعات خبراء الوايبو ومنظمة اليونسكو عامي 1983 و1985 التي أسفرت عن توجه عام لأعتبارها من قبيل الأعمال الأدبية، كما إن إتفاقية تربس إذ اعتبرتها كذلك وإضافتها إلى المصنفات الأدبية والفنية محل الحماية بموجب إتفاقية بيرن (م 1/10) فيكون الأتجاه الدولي قد حسم لصالح هذا الموقف.

وفق إتفاقية تربس فإن البرمجيات محل للحماية سواء أكانت بلغة الآلة أم المصدر (م 1/10) ولمؤلفها كافة الحقوق المالية والمعنوية لمصنفات حق المؤلف إضافة إلى حقه في أجازة أو منع تأجيرها– شأنها شأن التسجيلات الصوتية والمرئية (م 11)، ويستثنى وفق هذه المادة حالة التأجير التي لا يكون فيها البرنامج الموضوع الأساسي للتأجير. وأما بخصوص مدة الحماية فإنها تمتد إلى 50 عاماً محسوبة على أساس حياة الشخص الطبيعي فإن لم تكن كذلك فمن نهاية السنة التي أجيز فيها النشر أو تم فيها إنتاج العمل (م 12 تربس).

قواعد البيانات هي تجميع مميز للبيانات يتوافر فيه عنصر الأبتكار أو الترتيب أو التبويب عبر مجهود شخصي بأي لغة أو رمز ويكون مخزناً بواسطة الحاسوب ويمكن إسترجاعه بواسطتها أيضاً.

ومناط حماية قواعد البيانات – بوجه عام – هو البتكار كما عبرت عنه الإتفاقيات الدولية في هذا الحقل:

- فالمادة 2/10 من إتفاقية تربس نصت على أنه: تتمتع بالحماية البيانات المجمعة أو المواد الأخرى سواء كانت في شكل مقروء آلياً أو أي شكل آخر إذا كانت تشكل خلقاً فكرياً نتيجة إنتفاء وترتيب محتواها.
- كما نصت المادة 5 من الإتفاقية العالمية للملكية الفكرية لسنة 1996 – التي نفذت مؤخراً – على أنه: تتمتع مجموعات البيانات أو المواد الخرى بالحماية بصفتها هذه أيا كان شكلها إذا كانت تعتبر إبتكارات فكرية بسبب محتواها أو ترتيبها.
- لكن لا تجرى كافة النظم القانونية والقوانين على هذا النهج، فالتوجيهات الصادرة عن الإتحاد الوروبي في 1996/3/11 والقانون الفرنسي الصادر في عام 1998 لا يشترطان الأبتكار لحماية قواعد البيانات، بل يكفي ما بذل من جهد مالى أو بشري أو مادي وما أنفق من أجل إعداد قاعدة البيانات وسنداً لذلك فإن القانون الفرنسي المشار إليه يحمي قواعد البيانات لمدة خمس عشرة سنة ويحظر أي إعادة إستعمال سواء لجزء أو لمادة كلية من قاعدة البيانات عن طريق توزيع نسخ أو الإيجار أو النقل على الخط ويحظر النقل الكلي أو الجزئي – الجوهري – من محتوى قاعدة البيانات بأي شكل، متى كان الحصول أو تقديم هذا المحتوى قد أستلزم أستثمارات جوهرية كماً وكيفاً، وسواء أكان النقل دائماً ام مؤقتاً على دعامة بأي وسيلة أو تحت أي شكل.

والأبتكار يستمد إما من طبيعة البيانات نفسها وإما من طريقة ترتيبها أو إخراجها أو تجميعها أو إسترجاعها، ومحتوى البيانات في حد ذاته لا يعتبر عملاً إبتكارياً، ومن هنا فإن الأبتكار لا يتحقق إلا إذا عكست قاعدة البيانات سمات شخصية لواضعها.

- وقد قضت محكمة (نانت) التجارية الفرنسية في عان 1998 بأن الأبتكار الذي يتعلق بقاعدة بيانات على الإنترنيت يقتضي توافر جهد جاد في البحث والأختيار والتحليل والذي عندما يقارن بمجرد التوثيق تظهر أهمية الجهد المبتكر للعمل.
- أما قضاء محكمة النقض المصرية فإنه يتوسع في مفهوم الإبتكار، فقد قضت محكمة النقض المصرية عام 1964 بأن فهرسة إحدى كتب الأحاديث النبوية بعد عملاً إبتكارياً لأنه يكفي أن يكون عمل واضعه حديثاً في نوعه ويتميز بطابع شخص خاص وأنه يتعبر من قبل الأبتكار في الترتيب أو التنسيق أو بأي مجهود آخر أن يتسم بالطابع الشخصي.
- وعليه، فإن البيانات أو المعلومات المخزنة في نظم الحواسيب (بشكل مجرد) ليست محل حماية، كما بالنسبة للقوانين والأنظمة وقرارات القضاء مثلاً، لكنها متى ما أفرغت ضمن قاعدة بيانات وفق تصنيف معين وبآلية أسترجاع معين ومتى ما خضعت لعملية معالجة تتيح ذلك فإنها تتحول من مجرد بيانات إلى قاعدة معطيات، وينطوي إنجازها بهذا الوصف على جهد إبتكاري وإبداعي يستوجب الحماية، ويتزايد أهمية المعلومات، ولما حققته بنوك المعلومات من أهمية قصوى في الأعمال والنشاط الإنساني بوصفها أمست ذات قيمة مالية كبيرة بما تمثله، وباعتماد المشروعات عليها، ولتحول المعلومة إلى محدد إستراتيجي لرأس المال،بل البعض يراه مرتكزا لا محددا فقط ، نشط الاتجاه التشريعي في العديد من الدول لتوفير الحماية القانونية لقواعد البيانات. والأعتراف لقواعد البيانات بالحماية جاء وليد جهد واسع لمنظمة الوايبو ولمجلس أوربا الذي وضع عام 1996 قواعد إرشادية وقراراً يقضي بالنص على حماية قواعد البيانات ضمن قوانين حق المؤلف.

التحديات القانونية في حقل المعاملات الإلكترونية:

الأشكاليات القانونية التي صاحبت ظهور نظام المعاملات الإلكتررونية:

- كيفية إثبات الشخصية.
- كيفية التوقيع الإلكتروني.
- أنظمة الدفع النقدي الرقمي.
- المال الرقمي أو الإلكتروني أو القيدي.
- سرية وأمن المعلومات من مخاطر إجرام التقنية العالية.
- خصوصية العميل.
- المسئولية عن الأخطاء والمخاطر.
- حجية المراسلات الإلكترونية.
- التعاقدات المصرفية الإلكترونية.
- مسائل الملكية الفكرية لبرمجيات وقواعد معلومات البنك أو المستخدمة من موقع البنك أو المرتبطة بها.
- علاقات وتعاقدات البنك مع الجهات المزودة للتقنية أو الموردة لخدماتها أو مع المواقع الحليفة.
- مشاريع الأندماج والمشاركة والتعاون المعلوماتية.

هذه والكثير من التفرعات القانونية متواصل في الإطار القانوني للبنوك الإلكترونية والتجارة الإلكترونية والأعمال الإلكترونية والمعاملات الرقمية.

إن إنشاء المؤسسة بشكل فاعل على شبكة الإنترنت، يعنى أن:

- تحقق الوصول إلى أكبر قدر من العملاء.
- تحقق شمولية الخدمات المقدمة وتيسير قبولها وطلبها.

- تحقق قدراً متيقناً من أمن المعاملات وأمن إدارة أموال المساهمين.
- تحقيق قدراً مميزاً من كفاءة الخدمة المقدمة للعملاء وقدراً مقبولاً لحماية مصالح وأموال العملاء.

هذه العناصر الأربعة – التي يستلزم كل واحد منها خطة أداء وتميز – تكشف عبر التحليل الموضوعي عن حزمة من التحديات القانونية، وبقدر سلامة التعامل مع هذه التحديات بقدر ما تتحقق سلامة مرتكزات خطط تحقيق هذه العناصر وبقدر ما يصبح متاحاً بناء البنك الإلكتروني الحقيقي والمميز.

أما عن التحديات القانونية فهي تتمثل في:

١. تحدي قبول القانون للتعاقدات الإلكترونية.
٢. تحدي حجيتها في الإثبات.
٣. تحديات أمن المعلومات.
٤. تحديات وسائل الدفع الرقمية.
٥. تحديات الأعمال المرتبطة.
٦. تحديات المعايير والإشرافية "جهات الإشراف في حق البنوك الإلكترونية".
٧. التحديات الضريبية.

وسنتناول فيما يلي التحديات المرتبطة بالعمل المصرفي تحديداً والمرتبطة ببقية أنشطة الأعمال الإلكترونية:

تحديات التعاقدات الإلكترونية ومشكلات الإثبات:

يجب عدم الخلط بين مفهومين في حقل العقود وتقنية المعلومات:

أولاً: العقود التقليدية المبرمة بالوسائل الإلكترونية (ألتعاقد عبر شبكات المعلومات):

- أثارت وسائل الأتصال الحديث التساؤل حول مدى صحة أنعقاد العقد بواسطتها، كما في التلكس والفاكس، وتار في الوقت الحاضر – منذ مطلع التسعينات على الأقل.
- وما يتصل بها من حيث موثوقية وحجية الرسائل الإلكترونية والبريد الإلكتروني المتعلق بالعلاقات محل التعاقد.

- مسألة إثبات الأنعقاد ومسائل التعاقد (وقد أتجهت المواقف القانونية والقضائية والفقهية إلى قبول الوسائل التعاقدية التي توفر من حيث طبيعتها موثوقية في إثبات الواقعية وصلاحية الدليل محل الأحتجاج وتحقق فوق ذلك وظيفتين: إمكان حفظ المعلومات لغاية المراجعة عند التنازع، والتوسط في الإثبات عن طريق جهات الموثوقية الوسيطة أو سلطات الشهادات التعاقدية.

ثانياً: مسألة صحة الأنعقاد ووجوده، وتتصل هذه المسألة:

- بالإثبات على نحو يصعب كثيراً الفصل بينهما.
- إلى جانب مشكلات وأمن وسائل الأتصال.
- ودى قدرة الغير على التلاعب بالمحتوى.
- ومشكلات وقت ومكان الإبرام.
- واتصال ذلك بالقانون الواجب انطباقه على العقد عند المنازعة.
- وجهة الأختصاص القضائي في نظر النزاع.

– تعريف العقد الإلكتروني (التعاقد على الإنترنت):

إن العقد الإلكتروني هو أتفاق يتلاقي فيه الإيجاب والقبول على شبكة الإنترنت وذلك بوسيلة مسموعة أو مرئية ولا يختلف العقد الإلكتروني عن العقود التقليدية سوى في طريقة أنعقاد العقد وتنقسم الإلكترونية إلى قسمين:

الأول: هو العقد الإلكتروني الذي ينفذ على الإنترنت وذلك عندما تكون الخدمة المتفق عليها في العقد ليس لها وجود مادي مثل تقديم خدمة تصميم أو برمجة أو أستضافة أو دومين ومثل عقود الخدمات المصرفية بين البنك والعميل (البطاقات الأئتمانية)، وعقود الأستشارات القانونية بين المحامي وموكله، وعقود الأستشارات الطبية بين المؤسسات الطبية، وكل هه العقود بتم تنفيذها عن بعد عبر شبكة للأتصالات عن بعد. أي أن العقد يتم تنفيذه على الشبكة مباشرة.

أما القسم الثاني: فالإنترنت لا يكون إلا وسيلة للتعاقد عبره ولكن تنفيذ العقد يكون على أرض الواقع.

إن صحة التعبير عن الإدارة قد بنيت على العقد بالتراضي حسب أصل "التراضي في العقود"، وشروط صحة العقد لا تشمل على مراعاة رسميات معينة أو إستخدام لفظ خاص. على هذا الأساس لا مانع من التعبير عن الإدارة بصورة إلكترونية، إلا ان المشكلة تحدث عند ما تكون مراعاة رسميات معينة من شروط صحة العقد على وجه الإستثناء؛ على سبيل المثال حينما يعتبر التعبير عن الإدارة مرسوماً أو موقعاً، أمراً ضرورياً. بما أن الرسالة الإلكترونية لا يعتبر مرسوماً أو توقيعاً، اضطرت التجارة الإلكترونية أن تعتبر الرسالة الإلكترونية توقيعاً أو مكتوباً. من حيث تكوين التوافق، تنقذ القواعد العامة السائدة على العقود في هذا النوع من العقوم متى ما تكون ملائمة والعقود الإلكترونية.

– لتفادي المشكلات التي قد تنشأ عند تنفيذ العقود الإلكترونية يُنصح بما يلي:

- دقة صياغة العقل بأستخدام ألفاظ تتسم بالإحكام والإنضباط وتجنب الأللفاظ المرنة قدر الإمكان، بحيث تعبر الصياغة عن نية ومراد الطراف على نحو بيّن وواضح.
- تحديد العناصر الجوهيرة مثل محل العقد من حيث مشروعيته، ومن حيث الألتزامات التعلقة به من تسليم وضمان، والمقابل من حيث كيفية الوفاء، ونوع العملة، لما ينطوي عليه السداد الإلكتروني من مغالطات. بالإضافة إلى كافة الشروط المتفق عليها، والحقوق والألتزامات، والضمانات.
- تحديد القانون الواجب التطبيق، إذ يجب تحديد القانون الواجب التطبيق على العقد بدقة، تجنباً للدخول في تعقيدات القضاء من حيث تكييف العقد لتحديد القاون الواجب التطبيق.
- كما يكون شمول العقد لبديل آخر لحل المشكلات التي قد تنشأ وهو التحكيم الإلكتروني، الذي يتم فيه وضع إجراءات التحكيم وتبادل الوثائق إلكترونياً، وإصدار الأحكام التي قد تكون نافذة في حق الأطراف في ضوء الإجراءات التي تم الأتفاق عليها.
- تحديد المستندات التي تكون جزءاً من العقد مثل الرسائل الإلكترونية والمطبوعات المتبادلة بين الأطراف التي أفضت إلى التعاقد.